

Ser. No. 09/817,320

PATENT  
2001P04781US

## REMARKS

Claims 1, 2, 8, 12-16 and 20-22 are amended to correct formality errors and to more clearly define the invention.

Support for the amendments is found in the existing claims and in the Application description in connection with Figure 2 on pages 10-13 and specifically on page 10 lines 22-37 and other places.

*I. Rejection of claims 12 under 35 USC 112.*

Claim 12 is rejected under 35 USC 112 first paragraph as being non-enabling for encryption using RSA triple DES. The Rejection acknowledges that the specification is enabling for the MD5 algorithm

Claim 12 is amended to recite the "RSA (Rivest Shamir Adleman) MD5 compatible algorithm" acknowledged to be supported in the specification. Consequently this ground of rejection is no longer deemed to apply and its withdrawal is respectfully requested.

*II. Rejection of claim 2 under 35 USC 112.*

Claim 2 is rejected under 35 USC 112 second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter. Specifically, claim 2 language reciting "whichever comes first" is indefinite.

Claim 2 is amended to recite "said link processor adaptively identifies said address portion as URL data either, (a) lying between "http://" and a question mark "?" or (b) lying between "http://" and a pound/number sign "#", in response to whichever of condition (a) and (b) is satisfied first". As such the claim clarifies that the link processor identifies an address portion in response to whichever of condition (a) or (b) occurs first and is no longer indefinite. Consequently this ground of rejection is no longer deemed to apply and its withdrawal is respectfully requested.

*III. Rejection under 35 U.S.C. 102(e)*

Ser. No. 09/817,320

PATENT  
2001P04781US

Claims 1-11 and 13-22 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent 6,463,533 – Calamera et al. These claims, as amended, are deemed to be patentable for the reasons given below.

Amended claim 1 recites a system “employed by an application for encoding URL link data for use in detecting unauthorized URL modification” comprising “a link processor for processing URL data by identifying an address portion of said URL, encrypting said address portion of said URL, incorporating, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string; providing a key supporting decryption of said encrypted address portion to a destination system; and a communication processor for incorporating said processed URL data string into formatted data for communication to said destination system”. These features are not shown (or suggested) in Calamera.

The system of claim 1 involves “encrypting said address portion of said URL, incorporating, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string”. As well as “providing a key supporting decryption of said encrypted address portion, to a destination system”, for use in decrypting the “encrypted address portion” by the “destination system”. These features address the security deficiencies of URL processing functions of electronic systems. “Applications are vulnerable to the corruption of URL data and the context information conveyed within the URL data. The URL data conveyed from application 200 to application 230 includes context information comprising a session identifier and optionally a user or patient identifier. This URL data is potentially vulnerable to corruption to cause URL replay or redirection of an application to a substitute address or to gain access to application functions and parameters for unauthorized purposes. In order to protect against such corruption and to ensure that the entity being accessed is the one originally targeted, portions of the URL data conveyed between applications are advantageously encrypted” (Application page 11 lines 1-9).

The claimed system addresses the security problem by ensuring “that a URL link (e.g. a URL link to child application 230) embedded in a web page provided for display using browser 10 is not redirected. For this purpose, application 200 generates a hash value from the domain, path, program, and program data portion of the URL. Application 200 (as the sending application) generates a hash value from the fully qualified URL link” (Application page 9 lines 32-37). “Application 230

Ser. No. 09/817,320

PATENT  
2001P04781US

decrypts the received hash value for comparison with a corresponding hash value independently generated from corresponding URL data retrieved from a web server". Specifically, the "independently generated hash value and the hash value received by application 230 from application 200 via browser 10 are compared and if they are not equal, the request to initiate application 230 is rejected" (Application page 10 lines 25-37).

Calamera does not show or suggest "encrypting said address portion of said URL, incorporating, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string" for decryption by a "destination system" using the provided "key supporting decryption of said encrypted address portion". In Calamera, "in one embodiment of the invention, a one-way hash function is used to generate a site-specific user alias based on the user's identification code and the URL of the website. In an alternative embodiment of the invention, both a one-way hash function and a secret key encryption algorithm are used to generate the site-specific alias" (Calamera column 7 lines 1-7). Calamera generates a user specific alias code for insertion in an HTTP header in a GET request or in an HTTP GET request itself (Calamera column 12 lines 56-60, column 13 lines 17-21, Figure 7 step 126, Figure 8 step 230). Specifically,

Calamera generates the Alias code in a **first** method as: "one-way hash encryption"  $ALIAS = H(DOMAIN, PATH, ID, RANDOM)$   
Where:  $H(x)$  = one-way MD5 hash of " $x$ " and: DOMAIN = URL Internet domain name of the website being accessed PATH = URL path of the website being accessed ID = user identification code RANDOM = random data string associated with the user" (Calamera column 7 lines 42-55).

Calamera generates the Alias code in a **second** method as:  $ALIAS = E[KEY_{SITE}](ID, RANDOM, CHECKSUM), DOMAIN, PATH$   
Where: "secret key encryption"  $KEY_{SITE}$  = first 56 bits of:  $H(DOMAIN, PATH, KEY_{SYSTEM})$   $CHECKSUM = H(ID, RANDOM)$   
 $H(x)$  = one-way MD5 hash of " $x$ "  $E[k](m)$  = DES encryption of " $m$ " using secret key " $k$ " and: ID = user identification code  $KEY_{SYSTEM}$  = secret encryption key held by the operator of the alias server system DOMAIN = URL internet domain name of the web site being accessed PATH = URL path of the web site being accessed RANDOM = random data string associated with the user. Note that  $KEY_{SITE}$ , the encryption key used to generate the site-specific alias, is an encryption of a secret key with the URL of the website" (Calamera column 8 line 61 to column 9 line 15).

Ser. No. 09/817,320

PATENT  
2001P04781US

Both the first and second Calamera methods provide "a user specific alias code" for incorporation in a HTTP GET request in an encoded form. The first Calamera method provides a hashed code and the second method provides an encrypted code. However neither method shows or suggests "incorporating" an encrypted "address portion of said URL" in a URL for decryption by a "destination system" using the provided "key supporting decryption of said encrypted address portion".

In Calamera, a target system, upon receiving a URL request, can use the encrypted string and compare it to some known set of allowable strings in order to identify a user. However the target system **cannot decrypt** the encrypted string. "Regardless of when the alias is generated or how it is sent to the website accessed by the user, the alias maintains the user's anonymity since it is impractical to determine the user's identity from the alias. Nevertheless, because a user's alias for a particular website does not change over time, the website is able to recognize a particular user from previous occasions when the user accessed the website...Furthermore, since the alias server system can decrypt the alias to determine the user's identity, law enforcement agencies can obtain the user's identity from the operator of the alias server system if necessary" (Calamera column 11 lines 4-16). Consequently, the target system is unable to decrypt (nor has access to the necessary key for decrypting) the encrypted string. Only the source (alias server) system is able to decrypt.

In contrast, in the claimed arrangements, a target system has access to the key used by the generation system so that the data can be decrypted. Specifically, the claimed arrangement involves "providing a key supporting decryption of said encrypted address portion, to a destination system", for use in decrypting the "encrypted address portion" by the "destination system" for "use in detecting unauthorized URL modification". The Calamera system deliberately excludes the target system from decrypting the encrypted URL data (and does not provide the necessary key for decrypting). Only the source (alias server and alias code generation system) is able to decrypt. Further, the claimed arrangement enables additional contextual data to be conveyed to, and used by, the target system (e.g. patient identifier, encounter identifier, and so on). This is done by including the contextual data in the encrypted string for use by the target system (claims 8, 10, 11, 18 and 19). In the Calamera system such information cannot be conveyed for decryption and subsequent use. Calamera also has no notion of session. In contrast to the claimed

Ser. No. 09/817,320

PATENT  
2001P04781US

system, the Calamera system does NOT convey information in URL data fields for subsequent decryption and use by a target system.

Further, since the purpose of the Calamera encryption system is to allow "a computer network site, such as an Internet website, to recognize an anonymous user without revealing the identity of the user", there is no reason, problem recognition or motivation for amending the Calamera system to include the claimed arrangement (Calamera column 3 lines 6-10). Indeed, modification of the Calamera system to include such a feature would be in **direct conflict** with the teaching and objective of Calamera of maintaining a "user's anonymity since it is impractical to determine the user's identity from the alias" (Calamera column 11 lines 4-16). Consequently, withdrawal of the rejection of amended claim 1 under 35 USC 102(e) is respectfully requested.

Amended dependent claim 2 is considered to be patentable based on its dependence on claim 1. Claim 2 is also considered to be patentable because Calamera does not show (or suggest) a "link processor" that "adaptively identifies said address portion as URL data either, (a) lying between "http://" and a question mark "?" or (b) lying between "http://" and a pound/number sign "#", in response to whichever of condition (a) and (b) is satisfied first". Contrary to the Rejection statement on page 4, Calamera in column 7 lines 32-34 does not provide any 35 USC 112 compliant enabling description of adaptively identifying an "address portion" of a URL based on "whichever" of a "condition (a) and (b) is satisfied first". Specifically, adaptively identifying an "address portion" as URL data either, (a) lying between "http://" and a question mark "?" or (b) lying between "http://" and a pound/number sign "#", response to whichever of condition (a) and (b) is satisfied first". Calamera also shows no recognition of the problem this feature addresses.

Dependent claim 3 is considered to be patentable based on its dependence on claim 1. Claim 3 is also considered to be patentable because Calamera does not show (or suggest) "adaptively" identifying the "address portion based on the application associated with said URL". Contrary to the Rejection statement on page 4, Calamera in column 7 lines 32-34 does not provide any 35 USC 112 compliant enabling description of such a feature.

Dependent claim 4 is considered to be patentable based on its dependence on claims 1 and 3. Claim 4 is also considered to be patentable because Calamera does not show (or suggest) a "link processor" that "adaptively uses (a) an

Ser. No. 09/817,320

PATENT  
2001P04781US

address portion for ASP (Active Server Page) applications comprising a SERVER\_NAME and SCRIPT\_NAME and (b) an address portion for a non-ASP applications comprising a SERVER\_NAME, SCRIPT\_NAME, and PATH\_INFO". Contrary to the Rejection statement on page 4, Calamera in column 7 lines 32-34 does not provide any 35 USC 112 compliant enabling description of such a feature. Calamera fails to recognize any need for adaptive URL generation responsive to whether an Active Server Page is involved or not. Calamera does not mention use of Active Server Pages at all.

Dependent claim 5 is considered to be patentable based on its dependence on claim 1 and for reasons given in connection with claim 1.

Dependent claim 6 is considered to be patentable based on its dependence on claim 1. Claim 6 is also considered to be patentable because Calamera does not show (or suggest) a "link processor" that "converts said address portion of said URL to lower case before compression". Contrary to the Rejection statement on page 4, Calamera in column 8 lines 48-52 does not provide any 35 USC 112 compliant enabling description of such a feature. Calamera fails to recognize any need for case sensitive conversion. Calamera does not mention lower case or upper case at all.

Dependent claim 7 is considered to be patentable based on its dependence on claim 1 and for reasons given in connection with claim 1.

Amended dependent claim 8 is considered to be patentable based on its dependence on claim 1. Claim 8 is also considered to be patentable because Calamera does not show (or suggest) use of a "link processor" that "incorporates at least one of, (a) a session identifier, identifying a particular session of user initiated operation of said application and (b) an encrypted patient identifier, into said processed URL data string". Contrary to the Rejection statement on page 4, Calamera in column 8 lines 52-58 does not provide any 35 USC 112 compliant enabling description of a link processor that "incorporates at least one of, (a) a session identifier, identifying a particular session of user initiated operation of said application and (b) an encrypted patient identifier, into said processed URL data string". The claimed arrangement involving providing a patient identifier for decryption and use by a target application would enable a target system access to patient identity or session identity information and undermine the anonymity objective of the Calamera system. In Calamera, a target system, upon receiving a URL request, can use the encrypted string and compare it to

Ser. No. 09/817,320

PATENT  
2001P04781US

some known set of allowable strings in order to identify a user. However the target system cannot decrypt the encrypted string. "Regardless of when the alias is generated or how it is sent to the website accessed by the user, the alias maintains the user's anonymity since it is impractical to determine the user's identity from the alias" (Calamera column 11 lines 4-16). Consequently, the target system is unable to decrypt (nor has access to the necessary key for decrypting) the encrypted string. Only the source (alias server) system is able to decrypt.

In the claimed arrangements, a target system has access to the key used by the generation system so that the data can be decrypted. Specifically, the claimed arrangement involves "providing a key supporting decryption of said encrypted address portion, to a destination system", for use in decrypting the "encrypted address portion" by the "destination system" for "use in detecting unauthorized URL modification". The Calamera system deliberately excludes the target system from decrypting the encrypted URL data (and does not provide the necessary key for decrypting). Only the source (alias server and alias code generation system) is able to decrypt. Further, the claimed arrangement enables additional contextual data to also be used by the target system (e.g. patient identifier, encounter identifier, and so on). This contextual data is included in the encrypted string for use by the target system. In the Calamera system such information cannot be conveyed for decryption and subsequent use. Calamera also has no notion of session. In contrast to the claimed system, the Calamera system does NOT suggest conveying information in URL data fields for subsequent decryption and use by a target system.

Dependent claim 9 is considered to be patentable based on its dependence on claims 1 and 8 for reasons given in connection with these claims. Claim 9 is also considered to be patentable because Calamera does not show (or suggest) a "link processor" that "incorporates said session identifier into said processed URL data string by formatting said session identifier into a data field including said session identifier and encrypted address separated by a colon (that is, session identifier:encrypted address)". Calamera does NOT contemplate session identification or session identifier processing at all.

Dependent claim 10 is considered to be patentable based on its dependence on claim 1. Claim 10 is also considered to be patentable because Calamera does not show (or suggest) a "link processor" that "concatenates said address portion of said URL together with **data associated with a personal record** to form a data element, and encrypts said data element for incorporation into said single

Ser. No. 09/817,320

PATENT  
2001P04781US

processed URL data string". The Calamera system deliberately excludes the target system from decrypting the encrypted URL data (and does not provide the necessary key for decrypting) and therefore does NOT suggest conveying **"data associated with a personal record"** to a "destination system" for decryption by the "destination system".

Dependent claim 11 is considered to be patentable based on its dependence on claims 1 and 10. Claim 11 is also considered to be patentable because Calamera does not show (or suggest) "said data associated with a personal record is at least one of, (a) a patient identifier, (b) a user identifier, (c) an encounter identifier and (d) an observation identifier". Calamera does not suggest such a feature combination for reasons given in connection with claims 1, 8 and 10.

Dependent claim 12 is considered to be patentable based on its dependence on claim 1.

Amended independent claim 13 recites a "system employed by an application for encoding URL link data for use in detecting unauthorized URL modification" comprising "a link processor for processing URL data by identifying an address portion of said URL, encrypting said address portion of said URL, incorporating, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form and a session identifier identifying a user session of computer operation, into a single processed URL data string; and a communication processor for incorporating said processed URL data string into formatted data for communication to a request device".

Amended claim 13 is considered to be patentable for the reasons given in connection with claims 1 and 8. Claim 13 is also considered to be patentable because Calamera does not show (or suggest) a feature combination including "a link processor for processing URL data" by "encrypting said address portion of said URL, incorporating, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form and a **session identifier** identifying a user session of computer operation, into a single processed URL data string". Calamera does not show (or suggest) a "link processor" that incorporates a "session identifier" into a "single processed URL data string". Calamera does NOT contemplate session identification or session identifier processing at all.

Ser. No. 09/817,320

PATENT  
2001P04781US

Amended dependent claim 14 is considered to be patentable based on its dependence on claim 13. Claim 14 is also considered to be patentable because Calamera does not show (or suggest) a "link processor" that "compresses said identified address portion and encrypts said compressed address portion of said URL to provide said encrypted address portion and said link processor converts said identified address portion to lower case prior to compressing said identified address portion using a hash function". Calamera does not suggest such a feature combination for reasons given in connection with claims 1 and 6.

Amended independent claim 15 recites a "system employed by an application for decoding URL link data encoded for use in detecting unauthorized URL modification" comprising "an input processor for receiving an encoded URL; a link processor for processing said encoded URL by identifying an encrypted address portion of said received encoded URL and a corresponding non-encrypted address portion of said received encoded URL, decrypting said encrypted address portion of said URL to provide a decrypted URL address portion, a validation processor for determining if said decrypted URL address portion has been subject to unauthorized modification by determining if said decrypted URL address portion is different to said corresponding non-encrypted address portion of said received encoded URL".

Amended claim 15 is considered to be patentable for the reasons given in connection with claim 1. Claim 15 is also considered to be patentable because Calamera does not show (or suggest) a feature combination that detects "unauthorized URL modification" by "decrypting said encrypted address portion of said URL to provide a decrypted URL address portion" and "determining if said decrypted URL address portion has been subject to unauthorized modification by determining if said decrypted URL address portion is different to said corresponding non-encrypted address portion of said received encoded URL". Calamera does not recognize the problem of "unauthorized URL modification" or provide any way of addressing such a problem. Calamera is concerned with the entirely different problem of "allowing a computer network site, such as an Internet website, to recognize an anonymous user without revealing the identity of the user" (Calamera column 3 lines 6-9). The Calamera system deliberately excludes the target system from decrypting the encrypted URL data (and does not provide the necessary key for decrypting). Only the source (alias server and alias code generation system) is able to decrypt. Consequently, Calamera does not show or suggest "decrypting said encrypted address portion of said URL to provide a decrypted URL address portion". Further, Calamera does not show or suggest (and is incapable of) "determining if said decrypted URL

Ser. No. 09/817,320

PATENT  
2001P04781US

address portion has been subject to unauthorized modification by determining if said **decrypted** URL address portion is **different** to said corresponding **non-encrypted** address portion of said received encoded URL".

Amended dependent claim 16 is considered to be patentable based on its dependence on claim 15. Claim 16 is also considered to be patentable because Calamera does not show (or suggest) a system in which "said decrypted URL address portion is a first hash value, and said validation processor, applies a hashing function to said corresponding non-encrypted address portion of said received encoded URL to provide a **comparison second hash value**, and compares said comparison second hash value with said first hash value, and upon a match determines a successful validation of said received encoded URL" indicating no "unauthorized URL modification". Calamera does not suggest such a feature combination or contemplate comparing hash values representing URL address portions. Calamera does not contemplate or provide any such system for determining "unauthorized URL modification" at all.

Dependent claim 17 is considered to be patentable based on its dependence on claim 15. Claim 17 is also considered to be patentable because Calamera does not show (or suggest) a system that "identifies and extracts a session identifier from a non-encrypted portion of said received encoded URL". As previously explained Calamera does not suggest such a feature combination or mention session identification at all.

Dependent claim 18 is considered to be patentable based on its dependence on claim 15 for reasons given in connection with claims 1, 8, 10 and 11.

Dependent claim 19 is considered to be patentable based on its dependence on claims 15 and 18 for reasons given in connection with claims 1, 8, 10 and 11.

Amended independent claim 20 is a method claim mirroring apparatus claim 1 and is considered to be patentable for the same reasons.

Amended independent claim 21 is a method claim mirroring apparatus claim 15 and is considered to be patentable for the same reasons.

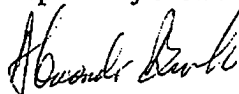
Ser. No. 09/817,320

PATENT  
2001P04781US

Amended dependent claim 22 is considered to be patentable based on its dependence on claim 21. Claim 22 is also considered to be patentable because of reasons given in connection with claims 15 and 16. Consequently, withdrawal of the rejection of claims 1-22 under 35 USC 102(e) is respectfully requested.

In view of the above amendments and remarks, Applicants submit that the Application is in condition for allowance, and favorable reconsideration is requested.

Respectfully submitted,



Alexander J. Burke

Reg. No. 40,425

Date: 29 November 2004

Alexander J. Burke  
Intellectual Property Department  
Siemens Corporation,  
170 Wood Avenue South  
Iselin, N.J. 08830  
Tel. 732 321 3023  
Fax 732 321 3030

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKewed/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**